CLAIMS

What is claimed is:

1. A method for secure remote mirroring of network traffic, the method comprising:

receiving a data packet to be remotely mirrored by an entry device pre-configured with a destination address to which to mirror the data packet;

encrypting the data packet to form an encrypted packet;

generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the destination address; and

forwarding the encapsulated encrypted packet to an exit device associated with the destination address.

2. The method of claim 1, wherein the destination address comprises an Internet protocol (IP) destination address, wherein the header comprises an IP header; and wherein the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet.

3. The method of claim 1, wherein the destination address comprises a media access control (MAC) destination address, and wherein the header comprises a MAC header, and wherein the encapsulated encrypted packet comprises a MAC-encapsulated encrypted packet.

4. The method of claim 2, further comprising:

determining a media access control (MAC) address associated with the destination IP address;

generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC address in a destination field; and

transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.

5. The method of claim 4, wherein determining the MAC address comprises:

determining if a mapping of the destination IP address to the MAC address is stored in an address resolution protocol (ARP) cache;
if so, then retrieving the MAC address from the ARP cache; and
if not, then broadcasting an ARP request with the destination IP address and receiving an ARP reply with the MAC address.

6. The method of claim 4, wherein the IP-encapsulated packet is communicated across multiple intermediate layer 2 domains.

7. The method of claim 1, further comprising:
receiving the encapsulated encrypted packet by the exit device;
removing the header to de-encapsulate the encrypted packet; and
decrypting the encrypted packet to re-generate the data packet.

8. The method of claim 7, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

9. The method of claim 8, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.

10. The method of claim 1, further comprising:
configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking.

11. The method of claim 1, further comprising:
configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic.

12. The method of claim 1, further comprising:
truncating the data packet to reduce a size of the data packet prior to encryption thereof.

13. The method of claim 1, further comprising:

compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption thereof.

14. A networking device comprising:

a plurality of ports for receiving and transmitting packets therefrom;

a secure remote mirroring engine configured to detect packets from a specified mirror source, to encrypt the detected packets, to encapsulate the encrypted packets, and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports; and

an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

15. The networking device of claim 14, wherein the destination comprises an Internet protocol (IP) destination address.

16. The networking device of claim 15, wherein the remote mirroring engine encrypts the packets using a public key of a public-private key pair.

17. A system for secure remote mirroring of network traffic, the system comprising:

a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, to encrypt the detected packets using an encryption module, encapsulate the encrypted packets, and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports; and

a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to decrypt the encrypted packets.

18. The system of claim 17, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

19. The system of claim 18, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.

20. A system for secure remote mirroring of network traffic, the system comprising a mirror entry device including means to encrypt the detected packets using an encryption module and to encapsulate the encrypted packets; and a mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to decrypt the encrypted packets.

21. A method for secure remote mirroring of network traffic, the method comprising:

remotely configuring an entry device with an encryption key and destination address;

remotely configuring an exit device at the destination address with a decryption key;

receiving a data packet to be mirrored by the entry device;

encrypting the data packet using the encryption key to form an encrypted packet;

generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the destination address; and

forwarding the encapsulated encrypted packet to the exit device.

22. The method of claim 21, wherein the remote configuration is performed by way of SNMP.

23. The method of claim 21, wherein the remote configuration is performed by way of a secure remote protocol.